

AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 850
OFFERED BY MR. TAUZIN OF LOUISIANA

Strike all after the enacting clause and insert the following:

1 SECTION 1. SHORT TITLE.

2 This Act may be cited as the “Security and Freedom
3 through Encryption (SAFE) Act”.

4 SEC. 2. DEFINITIONS.

5 For purposes of this Act, the following definitions
6 shall apply:

7 (1) COMPUTER HARDWARE.—The term “com-
8 puter hardware” includes computer systems, equip-
9 ment, application-specific assemblies, smart cards,
10 modules, integrated circuits, printed circuit board
11 assemblies, and devices that incorporate 1 or more
12 microprocessor-based central processing units that
13 are capable of accepting, storing, processing, or pro-
14 viding output of data.

15 (2) ENCRYPT AND ENCRYPTION.—The terms
16 “encrypt” and “encryption” means the scrambling
17 (and descrambling) of wire communications, elec-
18 tronic communications, or electronically stored infor-
19 mation, using mathematical formulas or algorithms

1 to preserve the confidentiality, integrity, or authen-
2 ticity of, and prevent unauthorized recipients from
3 accessing or altering, such communications or infor-
4 mation.

5 (3) ENCRYPTION PRODUCT.—The term
6 “encryption product”—

7 (A) means computer hardware, computer
8 software, or technology with encryption capa-
9 bilities; and

10 (B) includes any subsequent version of or
11 update to an encryption product, if the
12 encryption capabilities are not changed.

13 (4) KEY.—The term “key” means the variable
14 information used in a mathematical formula, code,
15 or algorithm, or any component thereof, used to
16 decrypt wire communications, electronic communica-
17 tions, or electronically stored information, that has
18 been encrypted.

19 (5) KEY RECOVERY INFORMATION.—The term
20 “key recovery information” means information that
21 would enable obtaining the key of a user of
22 encryption.

23 (6) PERSON.—The term “person” has the
24 meaning given the term in section 2510 of title 18,
25 United States Code.

1 (7) SECRETARY.—The term “Secretary” means
2 the Secretary of Commerce.

3 (8) STATE.—The term “State” means any
4 State of the United States and includes the District
5 of Columbia and any commonwealth, territory, or
6 possessions of the United States.

7 (9) UNITED STATES PERSON.—The term
8 “United States person” means any—

9 (A) United States citizen; or

10 (B) legal entity that—

11 (i) is organized under the laws of the
12 United States, or any States, the District
13 of Columbia, or any commonwealth, terri-
14 tory, or possession of the United States;
15 and

16 (ii) has its principal place of business
17 in the United States.

18 (10) WIRE COMMUNICATION; ELECTRONIC COM-
19 MUNICATION.—The terms “wire communication”
20 and “electronic communication” have the meanings
21 given such terms in section 2510 of title 18, United
22 States Code.

1 **SEC. 3. ENSURING DEVELOPMENT AND DEPLOYMENT OF**
2 **ENCRYPTION IS A VOLUNTARY PRIVATE SEC-**
3 **TOR ACTIVITY.**

4 (a) STATEMENT OF POLICY.—It is the policy of the
5 United States that the use, development, manufacture,
6 sale, distribution, and importation of encryption products,
7 standards, and services for purposes of assuring the con-
8 fidentiality, authenticity, or integrity of electronic infor-
9 mation shall be voluntary and market driven.

10 (b) LIMITATION ON REGULATION.—Neither the Fed-
11 eral Government nor a State may establish any conditions,
12 ties, or links between encryption products, standards, and
13 services used for confidentiality, and those used for au-
14 thenticity or integrity purposes.

15 **SEC. 4. PROTECTION OF DOMESTIC SALE AND USE OF**
16 **ENCRYPTION.**

17 Except as otherwise provided by this Act, it is lawful
18 for any person within any State, and for any United
19 States person in a foreign country, to develop, manufac-
20 ture, sell, distribute, import, or use any encryption prod-
21 uct, regardless of the encryption algorithm selected,
22 encryption length chosen, existence of key recovery, or
23 other plaintext access capability, or implementation or me-
24 dium used.

1 **SEC. 5. PROHIBITION ON MANDATORY GOVERNMENT AC-**
2 **CESS TO PLAINTEXT.**

3 (a) IN GENERAL.—No department, agency, or instru-
4 mentality of the United States or of any State may require
5 that, set standards for, condition any approval on, create
6 incentives for, or tie any benefit to a requirement that,
7 a decryption key, access to a key, key recovery informa-
8 tion, or any other plaintext access capability be—

9 (1) required to be built into computer hardware
10 or software for any purpose;

11 (2) given to any other person (including a de-
12 partment, agency, or instrumentality of the United
13 States or an entity in the private sector that may be
14 certified or approved by the United States or a
15 State); or

16 (3) retained by the owner or user of an
17 encryption key or any other person, other than for
18 encryption products for the use of the United States
19 Government or a State government.

20 (b) PROTECTION OF EXISTING ACCESS.—Subsection
21 (a) does not affect the authority of any investigative or
22 law enforcement officer, or any member of the intelligence
23 community (as defined in section 3 of the National Secu-
24 rity Act of 1947 (50 U.S.C. 401a)), acting under any law
25 in effect on the date of the enactment of this Act, to gain
26 access to encrypted communications or information.

1 **SEC. 6. UNLAWFUL USE OF ENCRYPTION IN FURTHERANCE**
2 **OF A CRIMINAL ACT.**

3 (a) ENCRYPTION OF INCRIMINATING COMMUNICA-
4 TIONS OR INFORMATION UNLAWFUL.—Any person who,
5 in the commission of a felony under a criminal statute of
6 the United States, knowingly and willfully encrypts in-
7 criminating communications or information relating to
8 that felony with the intent to conceal such communications
9 or information for the purpose of avoiding detection by
10 law enforcement agencies or prosecution—

11 (1) in the case of a first offense under this sec-
12 tion, shall be imprisoned for not more than 5 years,
13 or fined under title 18, United States Code, or both;
14 and

15 (2) in the case of a second or subsequent of-
16 fense under this section, shall be imprisoned for not
17 more than 10 years, or fined under title 18, United
18 States Code, or both.

19 (b) USE OF ENCRYPTION NOT A BASIS FOR PROB-
20 ABLE CAUSE.—The use of encryption by any person shall
21 not be the sole basis for establishing probable cause with
22 respect to a criminal offense or a search warrant.

23 **SEC. 7. EXPORTS OF ENCRYPTION.**

24 (a) AMENDMENT TO EXPORT ADMINISTRATION ACT
25 OF 1979.—Section 17 of the Export Administration Act

1 of 1979 (50 U.S.C. App. 2416) is amended by adding at
2 the end the following new subsection:

3 “(g) CERTAIN CONSUMER PRODUCTS, COMPUTERS,
4 AND RELATED EQUIPMENT.—

5 “(1) GENERAL RULE.—Subject to paragraphs
6 (2), (3), and (4), the Secretary shall have exclusive
7 authority to control exports of all computer hard-
8 ware, software, computing devices, customer prem-
9 ises equipment, communications network equipment,
10 and technology for information security (including
11 encryption), except that which is specifically de-
12 signed or modified for military use, including com-
13 mand, control, and intelligence applications.

14 “(2) CRITICAL INFRASTRUCTURE PROTECTION
15 PRODUCTS.—

16 “(A) IDENTIFICATION.—Not later than 90
17 days after the date of the enactment of the Se-
18 curity and Freedom through Encryption
19 (SAFE) Act, the Assistant Secretary of Com-
20 merce for Communications and Information and
21 the National Telecommunications and Informa-
22 tion Administration shall issue regulations that
23 identify, define, or determine which products
24 and equipment described in paragraph (1) are

1 designed for improvement of network security,
2 network reliability, or data security.

3 “(B) NTIA RESPONSIBILITY.—Not later
4 than the expiration of the 2-year period begin-
5 ning on the date of the enactment of the Secu-
6 rity and Freedom through Encryption (SAFE)
7 Act, all authority of the Secretary under this
8 subsection and all determinations and reviews
9 required by this section, with respect to prod-
10 ucts and equipment described in paragraph (1)
11 that are designed for improvement of network
12 security, network reliability, or data security
13 through the use of encryption, shall be exercised
14 through and made by the Assistant Secretary of
15 Commerce for Communications and Informa-
16 tion and the National Telecommunications and
17 Information Administration. The Secretary
18 may, at any time, assign to the Assistant Sec-
19 retary and the NTIA authority of the Secretary
20 under this section with respect to other prod-
21 ucts and equipment described in paragraph (1).

22 “(3) ITEMS NOT REQUIRING LICENSES.—After
23 a one-time, 15-day technical review by the Secretary,
24 no export license may be required, except pursuant
25 to the Trading with the Enemy Act or the Inter-

1 national Emergency Economic Powers Act (but only
2 to the extent that the authority of such Act is not
3 exercised to extend controls imposed under this Act),
4 for the export or reexport of—

5 “(A) any computer hardware or software
6 or computing device, including computer hard-
7 ware or software or computing devices with
8 encryption capabilities—

9 “(i) that is generally available;

10 “(ii) that is in the public domain for
11 which copyright or other protection is not
12 available under title 17, United States
13 Code, or that is available to the public be-
14 cause it is generally accessible to the inter-
15 ested public in any form; or

16 “(iii) that is used in a commercial,
17 off-the-shelf, consumer product or any
18 component or subassembly designed for
19 use in such a consumer product available
20 within the United States or abroad
21 which—

22 “(I) includes encryption capabili-
23 ties which are inaccessible to the end
24 user; and

1 “(II) is not designed for military
2 or intelligence end use;

3 “(B) any computing device solely because
4 it incorporates or employs in any form—

5 “(i) computer hardware or software
6 (including computer hardware or software
7 with encryption capabilities) that is ex-
8 empted from any requirement for a license
9 under subparagraph (A); or

10 “(ii) computer hardware or software
11 that is no more technically complex in its
12 encryption capabilities than computer
13 hardware or software that is exempted
14 from any requirement for a license under
15 subparagraph (A) but is not designed for
16 installation by the purchaser;

17 “(C) any computer hardware or software
18 or computing device solely on the basis that it
19 incorporates or employs in any form interface
20 mechanisms for interaction with other computer
21 hardware or software or computing devices, in-
22 cluding computer hardware and software and
23 computing devices with encryption capabilities;

24 “(D) any computing or telecommunication
25 device which incorporates or employs in any

1 form computer hardware or software encryption
2 capabilities which—

3 “(i) are not directly available to the
4 end user; or

5 “(ii) limit the encryption to be point-
6 to-point from the user to a central commu-
7 nications point or link and does not enable
8 end-to-end user encryption;

9 “(E) technical assistance and technical
10 data used for the installation or maintenance of
11 computer hardware or software or computing
12 devices with encryption capabilities covered
13 under this subsection; or

14 “(F) any encryption hardware or software
15 or computing device not used for confidentiality
16 purposes, such as authentication, integrity, elec-
17 tronic signatures, nonrepudiation, or copy pro-
18 tection.

19 “(4) COMPUTER HARDWARE OR SOFTWARE OR
20 COMPUTING DEVICES WITH ENCRYPTION CAPABILI-
21 TIES.—After a one-time, 15-day technical review by
22 the Secretary, the Secretary shall authorize the ex-
23 port or reexport of computer hardware or software
24 or computing devices with encryption capabilities for
25 nonmilitary end uses in any country—

1 “(A) to which exports of computer hard-
2 ware or software or computing devices of com-
3 parable strength are permitted for use by finan-
4 cial institutions not controlled in fact by United
5 States persons, unless there is substantial evi-
6 dence that such computer hardware or software
7 or computing devices will be—

8 “(i) diverted to a military end use or
9 an end use supporting international ter-
10 rorism;

11 “(ii) modified for military or terrorist
12 end use; or

13 “(iii) reexported without any author-
14 ization by the United States that may be
15 required under this Act; or

16 “(B) if the Secretary determines that a
17 computer hardware or software or computing
18 device offering comparable security is commer-
19 cially available outside the United States from
20 a foreign supplier, without effective restrictions.

21 “(5) DEFINITIONS.—For purposes of this
22 subsection—

23 “(A) the term ‘computer hardware’ has the
24 meaning given such term in section 2 of the Se-

1 curity and Freedom through Encryption
2 (SAFE) Act;

3 “(B) the term ‘computing device’ means a
4 device which incorporates one or more micro-
5 processor-based central processing units that
6 can accept, store, process, or provide output of
7 data;

8 “(C) the term ‘customer premises equip-
9 ment’ means equipment employed on the prem-
10 ises of a person to originate, route, or terminate
11 communications;

12 “(D) the term ‘data security’ means the
13 protection, through techniques used by indi-
14 vidual computer and communications users, of
15 data from unauthorized penetration, manipula-
16 tion, or disclosure;

17 “(E) the term ‘encryption’ has the mean-
18 ing given such term in section 2 of the Security
19 and Freedom through Encryption (SAFE) Act;

20 “(F) the term ‘generally available’ means,
21 in the case of computer hardware or computer
22 software (including computer hardware or com-
23 puter software with encryption capabilities)—

24 “(i) computer hardware or computer
25 software that is—

1 “(I) distributed through the
2 Internet;

3 “(II) offered for sale, license, or
4 transfer to any person without restric-
5 tion, whether or not for consideration,
6 including, but not limited to, over-the-
7 counter retail sales, mail order trans-
8 actions, phone order transactions,
9 electronic distribution, or sale on ap-
10 proval;

11 “(III) preloaded on computer
12 hardware or computing devices that
13 are widely available for sale to the
14 public; or

15 “(IV) assembled from computer
16 hardware or computer software com-
17 ponents that are widely available for
18 sale to the public;

19 “(ii) not designed, developed, or tai-
20 lored by the manufacturer for specific pur-
21 chasers or users, except that any such pur-
22 chaser or user may—

23 “(I) supply certain installation
24 parameters needed by the computer
25 hardware or software to function

1 properly with the computer system of
2 the user or purchaser; or

3 “(II) select from among options
4 contained in the computer hardware
5 or computer software; and

6 “(iii) with respect to which the manu-
7 facturer of that computer hardware or
8 computer software—

9 “(I) intended for the user or pur-
10 chaser, including any licensee or
11 transferee, to install the computer
12 hardware or software and has sup-
13 plied the necessary instructions to do
14 so, except that the manufacturer of
15 the computer hardware or software, or
16 any agent of such manufacturer, may
17 also provide telephone or electronic
18 mail help line services for installation,
19 electronic transmission, or basic oper-
20 ations; and

21 “(II) the computer hardware or
22 software is designed for such installa-
23 tion by the user or purchaser without
24 further substantial support by the
25 manufacturer;

1 “(F) the term ‘network reliability’ means
2 the prevention, through techniques used by pro-
3 viders of computer and communications serv-
4 ices, of the malfunction, and the promotion of
5 the continued operations, of computer or com-
6 munications network;

7 “(G) the term ‘network security’ means
8 the prevention, through techniques used by pro-
9 viders of computer and communications serv-
10 ices, of authorized penetration, manipulation, or
11 disclosure of information of a computer or com-
12 munications network;

13 “(H) the term ‘technical assistance’ in-
14 cludes instruction, skills training, working
15 knowledge, consulting services, and the transfer
16 of technical data;

17 “(I) the term ‘technical data’ includes
18 blueprints, plans, diagrams, models, formulas,
19 tables, engineering designs and specifications,
20 and manuals and instructions written or re-
21 corded on other media or devices such as disks,
22 tapes, or read-only memories; and

23 “(J) the term ‘technical review’ means a
24 review by the Secretary of computer hardware
25 or software or computing devices with

1 encryption capabilities, based on information
2 about the product's encryption capabilities sup-
3 plied by the manufacturer, that the computer
4 hardware or software or computing device
5 works as represented.”.

6 (b) TRANSFER OF AUTHORITY TO NATIONAL TELE-
7 COMMUNICATIONS AND INFORMATION ADMINISTRA-
8 TION.—Section 103(b) of the National Telecommuni-
9 cations and Information Administration Organization Act
10 (47 U.S.C. 902(b)) is amended by adding at the end the
11 following new paragraph:

12 “(4) EXPORT OF COMMUNICATIONS TRANS-
13 ACTION TECHNOLOGIES.—In accordance with section
14 17(g)(2) of the Export Administration Act of 1979
15 (50 U.S.C. App. 2416(g)(2)), the Secretary shall as-
16 sign to the Assistant Secretary and the NTIA the
17 authority of the Secretary under such section 17(g),
18 with respect to products and equipment described in
19 paragraph (1) of such section that are designed for
20 improvement of network security, network reliability,
21 or data security, that (after the expiration of the 2-
22 year period beginning on the date of the enactment
23 of the Security and Freedom through Encryption
24 (SAFE) Act) is to be exercised by the Assistant Sec-
25 retary and the NTIA.”.

1 (c) NO REINSTATEMENT OF EXPORT CONTROLS ON
2 PREVIOUSLY DECONTROLLED PRODUCTS.—Any
3 encryption product not requiring an export license as of
4 the date of enactment of this Act, as a result of adminis-
5 trative decision or rulemaking, shall not require an export
6 license on or after such date of enactment.

7 (d) APPLICABILITY OF CERTAIN EXPORT CON-
8 TROLS.—

9 (1) IN GENERAL.—Nothing in this Act shall
10 limit the authority of the President under the Inter-
11 national Emergency Economic Powers Act, the
12 Trading with the Enemy Act, or the Export Admin-
13 istration Act of 1979, to—

14 (A) prohibit the export of encryption prod-
15 ucts to countries that have been determined to
16 repeatedly provide support for acts of inter-
17 national terrorism; or

18 (B) impose an embargo on exports to, and
19 imports from, a specific country.

20 (2) SPECIFIC DENIALS.—The Secretary of
21 Commerce may prohibit the export of specific
22 encryption products to an individual or organization
23 in a specific foreign country identified by the Sec-
24 retary, if the Secretary determines that there is sub-

1 stantial evidence that such encryption products will
2 be used for military or terrorist end-use.

3 (3) DEFINITION.—As used in this subsection
4 and subsection (c), the term “encryption” has the
5 meaning given that term in section 17(g)(5) of the
6 Export Administration Act of 1979, as added by
7 subsection (a) of this section.

8 (e) CONTINUATION OF EXPORT ADMINISTRATION
9 ACT.—For purposes of carrying out the amendment made
10 by subsection (a), the Export Administration Act of 1979
11 shall be deemed to be in effect.

12 **SEC. 8. GOVERNMENT PROCUREMENT OF ENCRYPTION**
13 **PRODUCTS.**

14 (a) STATEMENT OF POLICY.—It is the policy of the
15 United States—

16 (1) to permit the public to interact with govern-
17 ment through commercial networks and infrastruc-
18 ture; and

19 (2) to protect the privacy and security of any
20 electronic communication from, or stored informa-
21 tion obtained from, the public.

22 (b) PURCHASE OF ENCRYPTION PRODUCTS BY FED-
23 ERAL GOVERNMENT.—Any department, agency, or instru-
24 mentality of the United States may purchase encryption
25 products for internal use by officers and employees of the

1 United States to the extent and in the manner authorized
2 by law.

3 (c) PROHIBITION OF REQUIREMENT FOR CITIZENS
4 TO PURCHASE SPECIFIED PRODUCTS.—No department,
5 agency, or instrumentality of the United States, nor any
6 department, agency, or political subdivision of a State,
7 may require any person in the private sector to use any
8 particular encryption product or methodology, including
9 products with a decryption key, access to a key, key recovery
10 information, or any other plaintext access capability,
11 to communicate with, or transact business with, the gov-
12 ernment.

13 **SEC. 9. NATIONAL ELECTRONIC TECHNOLOGIES CENTER.**

14 Part C of the National Telecommunications and In-
15 formation Administration Organization Act is amended by
16 inserting after section 155 (47 U.S.C. 904) the following
17 new section:

18 **“SEC. 106. NATIONAL ELECTRONIC TECHNOLOGIES CEN-**
19 **TER.**

20 “(a) ESTABLISHMENT.—There is established in the
21 NTIA a National Electronic Technologies Center (in this
22 section referred to as the ‘NET Center’).

23 “(b) DIRECTOR.—The NET Center shall have a Di-
24 rector, who shall be appointed by the Assistant Secretary.

1 “(c) DUTIES.—The duties of the NET Center shall
2 be—

3 “(1) to serve as a center for industry and gov-
4 ernment entities to exchange information and meth-
5 odology regarding data security techniques and tech-
6 nologies;

7 “(2) to examine encryption techniques and
8 methods to facilitate the ability of law enforcement
9 to gain efficient access to plaintext of communica-
10 tions and electronic information;

11 “(3) to conduct research to develop efficient
12 methods, and improve the efficiency of existing
13 methods, of accessing plaintext of communications
14 and electronic information;

15 “(4) to investigate and research new and
16 emerging techniques and technologies to facilitate
17 access to communications and electronic informa-
18 tion, including —

19 “(A) reverse-steganography;

20 “(B) decompression of information that
21 previously has been compressed for trans-
22 mission; and

23 “(C) de-multiplexing;

24 “(5) to obtain information regarding the most
25 current computer hardware and software, tele-

1 communications, and other capabilities to under-
2 stand how to access information transmitted across
3 computer and communications networks; and

4 “(6) to serve as a center for Federal, State, and
5 local law enforcement authorities for information
6 and assistance regarding decryption and other access
7 requirements.

8 “(d) EQUAL ACCESS.—State and local law enforce-
9 ment agencies and authorities shall have access to infor-
10 mation, services, resources, and assistance provided by the
11 NET Center to the same extent that Federal law enforce-
12 ment agencies and authorities have such access.

13 “(e) PERSONNEL.—The Director may appoint such
14 personnel as the Director considers appropriate to carry
15 out the duties of the NET Center.

16 “(f) ASSISTANCE OF OTHER FEDERAL AGENCIES.—
17 Upon the request of the Director of the NET Center, the
18 head of any department or agency of the Federal Govern-
19 ment may, to assist the NET Center in carrying out its
20 duties under this section—

21 “(1) detail, on a reimbursable basis, any of the
22 personnel of such department or agency to the NET
23 Center; and

24 “(2) provide to the NET Center facilities, infor-
25 mation, and other non-personnel resources.

1 “(g) PRIVATE INDUSTRY ASSISTANCE.—The NET
2 Center may accept, use, and dispose of gifts, bequests, or
3 devises of money, services, or property, both real and per-
4 sonal, for the purpose of aiding or facilitating the work
5 of the Center. Gifts, bequests, or devises of money and
6 proceeds from sales of other property received as gifts, be-
7 quests, or devises shall be deposited in the Treasury and
8 shall be available for disbursement upon order of the Di-
9 rector of the NET Center.

10 “(h) ADVISORY BOARD.—

11 “(1) ESTABLISHMENT.—There is established
12 the Advisory Board of the Strategic NET Center for
13 Excellence in Information Security (in this sub-
14 section referred to as the “Advisory Board”), which
15 shall be comprised of 11 members who shall have
16 the qualifications described in paragraph (2) and
17 who shall be appointed by the Assistant Secretary
18 not later than 6 months after the date of the enact-
19 ment of this Act. The chairman of the Advisory
20 Board shall be designated by the Assistant Secretary
21 at the time of appointment.

22 “(2) QUALIFICATIONS.—Each member of the
23 Advisory Board shall have experience or expertise in
24 the field of encryption, decryption, electronic com-

1 munication, information security, electronic com-
2 merce, or law enforcement.

3 “(3) DUTIES.—The duty of the Advisory Board
4 shall be to advise the NET Center and the Federal
5 Government regarding new and emerging tech-
6 nologies relating to encryption and decryption of
7 communications and electronic information.

8 “(i) IMPLEMENTATION PLAN.—Within 2 months
9 after the date of the enactment of this Act, the Assistant
10 Secretary, in consultation and cooperation with other ap-
11 propriate Federal agencies and appropriate industry par-
12 ticipants, develop and cause to be published in the Federal
13 Register a plan for establishing the NET Center. The plan
14 shall—

15 “(1) specify the physical location of the NET
16 Center and the equipment, software, and personnel
17 resources necessary to carry out the duties of the
18 NET Center under this section;

19 “(2) assess the amount of funding necessary to
20 establish and operate the NET Center; and

21 “(3) identify sources of probable funding for
22 the NET Center, including any sources of in-kind
23 contributions from private industry.”.

1 **SEC. 10. STUDY OF NETWORK AND DATA SECURITY ISSUES.**

2 Part C of the National Telecommunications and In-
3 formation Administration Organization Act is amended by
4 adding at the end the following new section:

5 **“SEC. 156. STUDY OF NETWORK RELIABILITY AND SECUR-**
6 **ITY AND DATA SECURITY ISSUES.**

7 “(a) IN GENERAL.—The NTIA shall conduct an ex-
8 amination of—

9 “(1) the relationship between—

10 “(A) network reliability (for communica-
11 tions and computer networks), network security
12 (for such networks), and data security issues;
13 and

14 “(B) the conduct, in interstate commerce,
15 of electronic commerce transactions, including
16 through the medium of the telecommunications
17 networks, the Internet, or other interactive
18 computer systems;

19 “(2) the availability of various methods for
20 encrypting communications; and

21 “(3) the effects of various methods of providing
22 access to encrypted communications and to informa-
23 tion to further law enforcement activities.

24 “(b) SPECIFIC ISSUES.—In conducting the examina-
25 tion required by subsection (a), the NTIA shall—

1 “(1) analyze and evaluate the requirements
2 under paragraphs (3) and (4) of section 17(g) of the
3 Export Administration Act of 1979 (50 U.S.C. App.
4 2416(g); as added by section 7(a) of this Act) for
5 products referred to in such paragraphs to qualify
6 for the license exemption or mandatory export au-
7 thorization under such paragraphs, and determine—

8 “(A) the scope and applicability of such re-
9 quirements and the products that, at the time
10 of the examination, qualify for such license ex-
11 emption or export authorization; and

12 “(B) the products that will, 12 months
13 after the examination is conducted, qualify for
14 such license exemption or export authorization;
15 and

16 “(2) assess possible methods for providing ac-
17 cess to encrypted communications and to informa-
18 tion to further law enforcement activities.

19 “(c) REPORTS.—Within one year after the date of en-
20 actment of this section, the NTIA shall submit to the Con-
21 gress and the President a detailed report on the examina-
22 tion required by subsections (a) and (b). Annually there-
23 after, the NTIA shall submit to the Congress and the
24 President an update on such report.

25 “(d) DEFINITIONS.—For purposes of this section—

1 “(1) the terms ‘data security’, ‘encryption’,
2 ‘network reliability’, and ‘network security’ have the
3 meanings given such terms in section 17(g)(5) of the
4 Export Administration Act of 1979 (50 U.S.C. App.
5 2416(g)(5)); and

6 “(2) the terms ‘Internet’ and ‘interactive com-
7 puter systems’ have the meanings provided by sec-
8 tion 230(e) of the Communications Act of 1934 (47
9 U.S.C. 230(e)).

10 **SEC. 11. TREATMENT OF ENCRYPTION IN INTERSTATE AND**
11 **FOREIGN COMMERCE.**

12 (a) INQUIRY REGARDING IMPEDIMENTS TO COM-
13 MERCE.—Within 180 days after the date of the enactment
14 of this Act, the Secretary of Commerce shall complete an
15 inquiry to—

16 (1) identify any domestic and foreign impedi-
17 ments to trade in encryption products and services
18 and the manners in which and extent to which such
19 impediments inhibit the development of interstate
20 and foreign commerce; and

21 (2) identify import restrictions imposed by for-
22 eign nations that constitute trade barriers to pro-
23 viders of encryption products or services.

24 The Secretary shall submit a report to the Congress re-
25 garding the results of such inquiry by such date.

1 (b) REMOVAL OF IMPEDIMENTS TO TRADE.—Within
2 1 year after such date of enactment, the Secretary shall
3 prescribe such regulations as may be necessary to reduce
4 the impediments to trade in encryption products and serv-
5 ices identified in the inquiry pursuant to subsection (a)
6 for the purpose of facilitating the development of inter-
7 state and foreign commerce. Such regulations shall be de-
8 signed to—

9 (1) promote the sale and distribution, including
10 through electronic commerce, in foreign commerce of
11 encryption products and services manufactured in
12 the United States; and

13 (2) strengthen the competitiveness of domestic
14 providers of encryption products and services in for-
15 eign commerce, including electronic commerce.

16 (c) INTERNATIONAL AGREEMENTS.—

17 (1) REPORT TO PRESIDENT.—Upon the comple-
18 tion of the inquiry under subsection (a), the Sec-
19 retary shall submit a report to the President regard-
20 ing reducing any impediments to trade in encryption
21 products and services that are identified by the in-
22 quiry and could, in the determination of the Sec-
23 retary, require international negotiations for such re-
24 duction.

1 (2) NEGOTIATIONS.—The President shall take
2 all actions necessary to conduct negotiations with
3 other countries for the purposes of (A) concluding
4 international agreements on the promotion of
5 encryption products and services, and (B) achieving
6 mutual recognition of countries' export controls, in
7 order to meet the needs of countries to preserve na-
8 tional security, safeguard privacy, and prevent com-
9 mercial espionage. The President may consider a
10 country's refusal to negotiate such international ex-
11 port and mutual recognition agreements when con-
12 sidering the participation of the United States in
13 any cooperation or assistance program with that
14 country. The President shall submit a report to the
15 Congress regarding the status of international ef-
16 forts regarding cryptography not later than Decem-
17 ber 31, 2000.

18 **SEC. 12. COLLECTION OF INFORMATION ON EFFECT OF**
19 **ENCIPHERMENT ON LAW ENFORCEMENT ACTIVI-**
20 **TIES.**

21 (a) COLLECTION OF INFORMATION BY ATTORNEY
22 GENERAL.—The Attorney General shall compile, and
23 maintain in classified form, data on the instances in which
24 encipherment (as defined in section 2801 of title 18, United
25 States Code) has interfered with, impeded, or obstructed

1 the ability of the Department of Justice to enforce the
2 criminal laws of the United States.

3 (b) AVAILABILITY OF INFORMATION TO THE CON-
4 GRESS.—The information compiled under subsection (a),
5 including an unclassified summary thereof, shall be made
6 available, upon request, to any Member of Congress.